2025 年 1 月 15 日

お客様各位

株式会社日立ソリューションズ
Fortinet 製品ユーザサポート

【脆弱性】FortiSwitch における許可されていないコード実行の脆弱性(CVE-2023-37936)について

拝啓、平素は Fortinet 製品サポートをご利用下さいまして誠にありがとうございます。

この度 Fortinet 社より、深刻度の高い脆弱性として、FortiSwitch に関する脆弱性(CVE-2023-37936)がアナウンスされています。本脆弱性の影響を受けるバージョンをご利用のお客様におかれましては、対策済み OS へのバージョンアップのご検討をお願いいたします。

敬具

記

1. 事象の概要

FortiSwitch において、ハードコードされた暗号鍵の利用に関する脆弱性[CWE-321]があり、外部の認証されていない攻撃者に、許可されていないコードを実行される可能性があります。

詳細、最新の情報については Fortinet 社から発表されています以下セキュリティアドバイザリ(PSIRT Advisories)をご覧ください。

Hardcoded Session Secret Leading to Unauthenticated Remote Code Execution
<https://www.fortiguard.com/psirt/FG-IR-23-260>

2. 該当製品と対策バージョン

弊社取り扱い済みの製品・バージョンにて、脆弱性の影響を受けるバージョン、及び対策バージョンは以下の通りです。

項	メジャーバージョン	影響を受けるバージョン	対策バージョン	備考
1	FortiSwitch 7.4 系	7.4.0	7.4.1 以降	7.4.0 は弊社未リリースのバージョン
2	FortiSwitch 7.2 系	7.2.5 以前	7.2.6 以降	
3	FortiSwitch 7.0 系	7.0.7 以前	7.0.8 以降	
4	FortiSwitch 6.4 系	6.4.13 以前	6.4.14 以降	EOS 済みバージョン

3. 回避策

影響を受けるバージョンを使用している場合は、対策バージョンへアップデートしてください。

4. OS ファイルの入手方法

バージョンアップは、対象機器がインターネットに接続している場合は、GUI で OS のダウンロード、及びバージョンアップを行うことができます。

OS ファイルがご入用の場合は、弊社サポートからご提供しております。対象機器のシリアル番号(S/N)と共に、現在のバージョン、バージョンアップ先のバージョンをご連絡ください。

5. Fortinet 社セキュリティアドバイザリ

Fortinet 社では、脆弱性情報を以下、FortiGuard Labs PSIRT Advisories で公開しています。最新の脆弱性情報は以下サイトをご覧頂き、適時ご利用環境の対策をいただきますようお願いします。

尚、同サイト記載内容以上の情報は開示されていません。記載内容の解釈また内容等については、弊社サポートではお答えいたしかねます。予めご了承ください。

PSIRT Advisories は RSS 配信も行われていますので、合わせてご活用ください。

FortiGuard Labs PSIRT Advisories
<https://www.fortiguard.com/psirt>

FortiGuard Labs RSS Feeds
<https://www.fortiguard.com/rss-feeds>

以上